2021年10月28日
第1回ブロックチェーンセキュリティワークショップ（ BWS2021）
基調講演 #2

暗号資産カストディアンとセキュリティ

株式会社メルコイン Security
中島 博敬

中島 博敬
(Hirotaka Nakajima)

@nunnun
@nunnun
nunnun@mercari.com

Title:

- Security Engineer at Mercoin, Inc.
- Site Reliability Engineer at Mercari, Inc.

Carrier:

- https://researchmap.jp/nunnun

Activities:

- 一般社団法人日本暗号資産取引業協会
  技術委員会 専門委員
- Cryptoasset Governance Task Force
  メンバー
- Internet Society Japan Chapter Treasury

Hobbies:

- インターネット運用 (AS63774)
- 旅行

メルカリとは

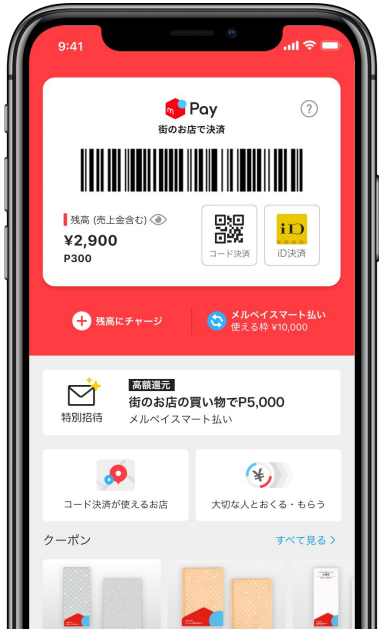
mercari

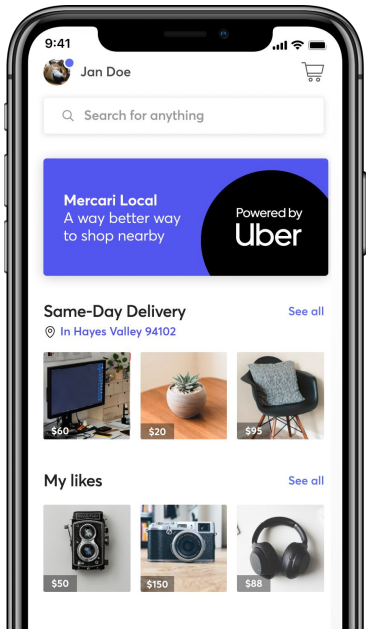
mercari

Pay

MERCARI

Shops





FACTBOOK

本日の流れ

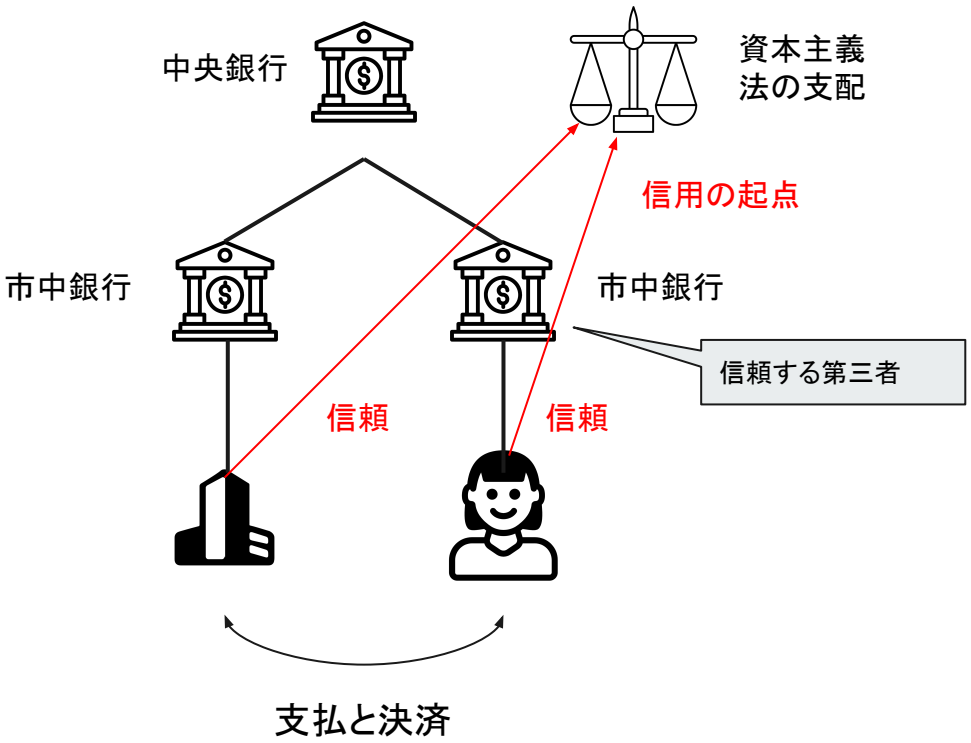
- 暗号資産交換所とカストディアンの関係
- 暗号資産セキュリティに取り組む活動の紹介
- 暗号資産の今後の課題
  - 暗号鍵管理
  - トラストアンカー

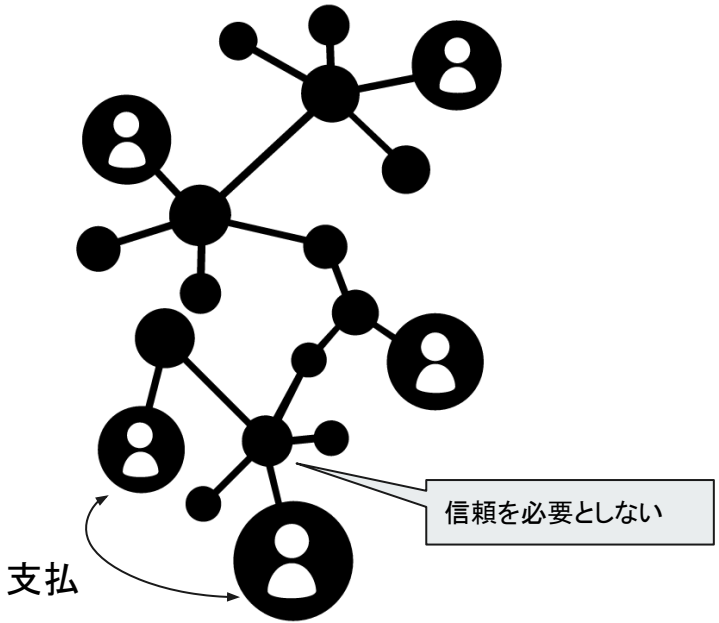
暗号資産とトラストレス

トラストレスの世界

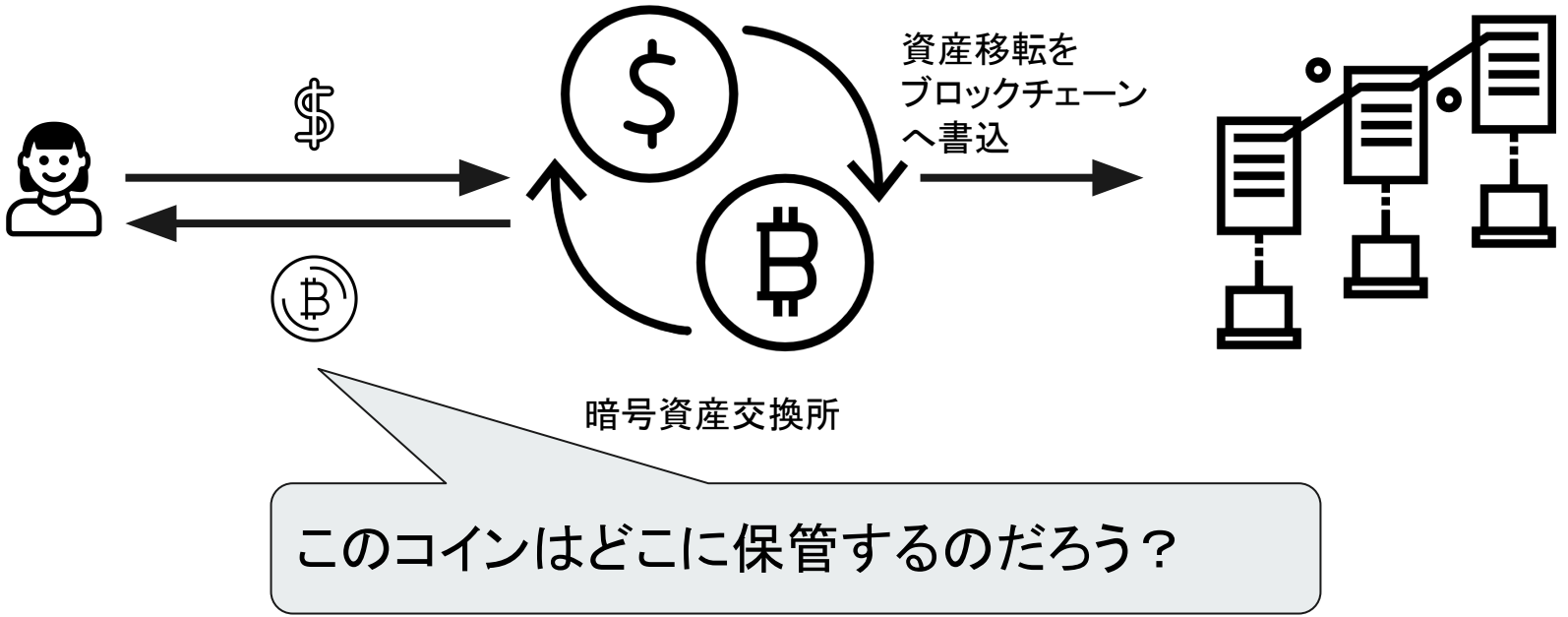
> *“SatoshiのPaperは、二重支払いの防止とPaymentの範囲であれば、Without Trusted Third Partyでもうまく回る、という世界の境界線を主張している。”*
> 松尾 真一郎, “Satoshiが注意深く設定した世界の境界線”, Online 2018

中央集権とトラストレス





暗号資産取引所



暗号資産の保管先

Hirotaka Nakajima
@nunnun

暗号資産をお持ちの方にお伺いしたいのですが、ご自身の資産はどのように管理されていらっしゃいますか？

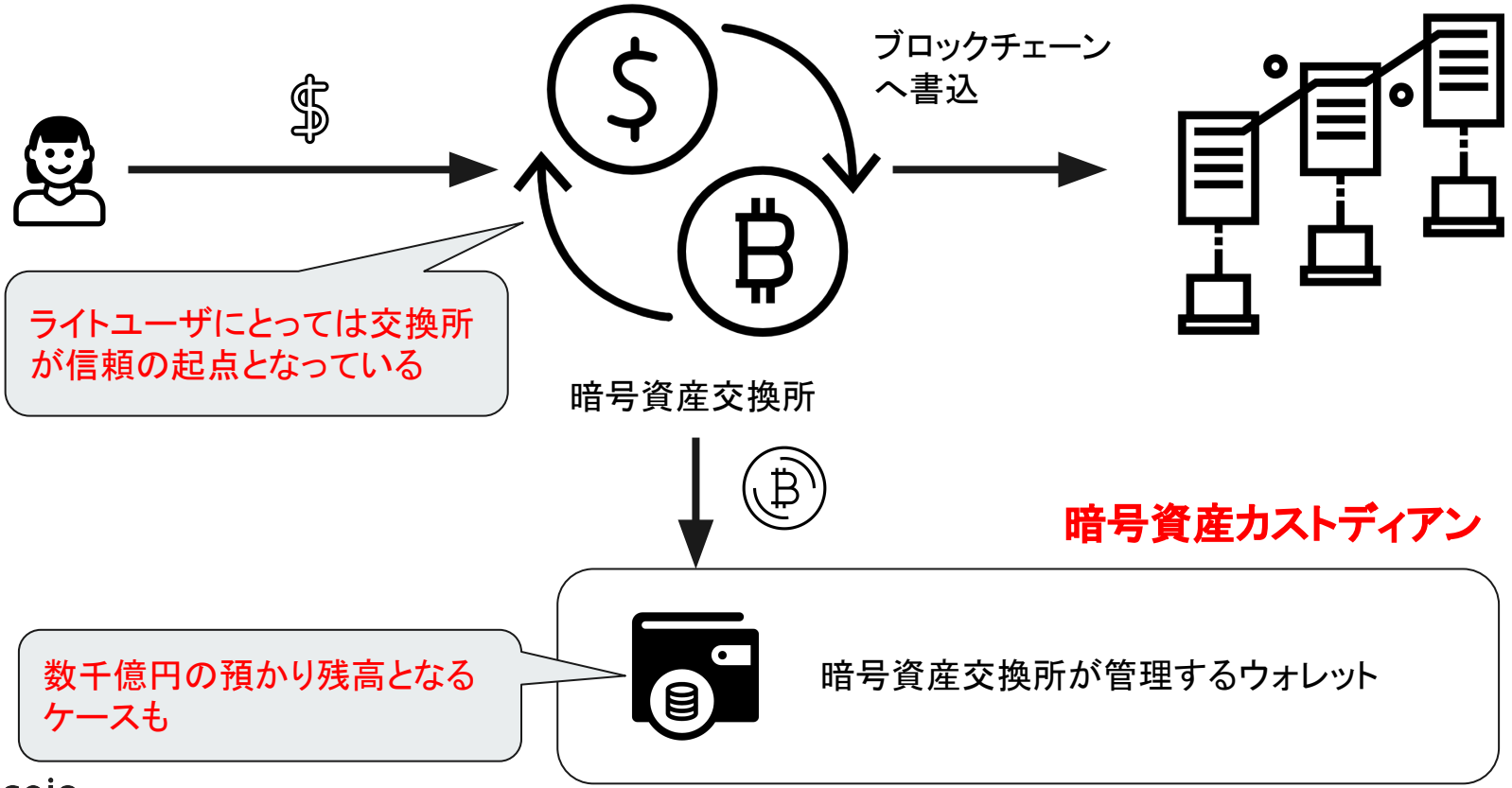
Translate Tweet

暗号資産取引所に預けている	45.9%
自身で管理している(ハードウェアウォレット等)	22.4%
その他	4.1%
結果だけ見たい	27.6%

98 votes · Final results

10:16 AM · Oct 14, 2021 · Twitter Web App

暗号資産取引所(実態)


ブロックチェーン
へ書込
ライトユーザにとっては交換所
が信頼の起点となっている
暗号資産交換所
暗号資産カストディアン
数千億円の預かり残高となる
ケースも
暗号資産交換所が管理するウォレット

暗号資産インシデント

- **Bithumb** - 2017年7月, 2018年6月, 2019年3月 [1][2][3,4,5]
  1. 内部犯による交換所資産の不正トランザクション
  2. 従業員のデバイスが侵害され、顧客情報が盗まれた後、資産流出。
  3. ホットウォレット上の資産が盗まれた。情報セキュリティ体制に問題があるとの指摘。
- **Coincheck** - 2018年1月 [1][2]
  攻撃者から送付されたメールに添付されたソフトウェアを実行してしまい、署名鍵が奪取されたことが原因とみられる。
- **BlackWallet** - 2018年1月 [1][2]
  DNSレコードが改ざんされ、移動先のアドレスが書き換えられてしまった
- **BitGrail** - 2018年2月 [1]
  顧客残高の検証機能に問題があり、残高不足でも引き出すことを可能としていた。
- **Taylor** - 2018年5月 [1][2]
  デバイスに対するアクセスを奪われ、1Passwordファイルを奪取されてしまった

暗号資産インシデントの原因

多くは原因が明らかではないが、いくつか共通する点が存在する

- **暗号資産交換所に対する標的型攻撃メール**
  フィッシング/標的型攻撃メールを用いて、従業員の PCに対するアクセスが奪われるケース。
  Bitstamp(2015), Bithumb(2017), Coincheck(2018)
- **従業員のクレデンシャルに対する攻撃**
  従業員のクレデンシャルが弱い、または安全でない方法でクレデンシャルが保存されていたケース。
  Bithumb(2017), NiceHash(2017), YouBit(2017)
- **システム脆弱性に対する攻撃**
  交換所システム及びソフトウェアの脆弱性を利用して不正に引き出しを行うケース。
  BitGrail(2018), Geth(2018), Bancor(2018)
- **ホットウォレットに対する攻撃**
  ホットウォレットの署名鍵そのものが奪取されるケース。
  Bitfinex(2016), Parity(2018), Taylor(2018), Coincheck(2018)

Cryptassets Governance Task Force

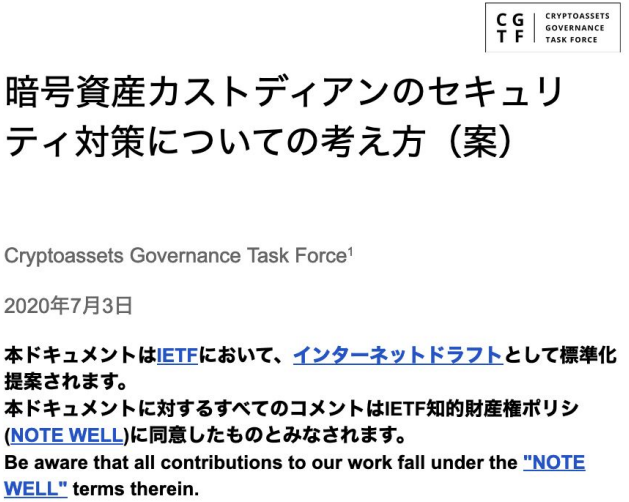
利用者保護のため、安全対策基準の策定に資する情報の提供を目的とした団体

- 主要メンバー
  - 岩下直行 (京都大学)、上原哲太郎 (立命館大学)、松尾真一郎 (ジョージタウン大学)
  - 楠正憲、松本泰、崎村夏彦
- 活動内容
  - 暗号資産(仮想通貨)交換所におけるセキュリティのベストプラクティスの基礎となる文書の作成
  - 暗号資産に関連した調査・研究の実施
- 運営ポリシー
  - 中立性・透明性・実効性
- 外部機関との連携
  - 標準化団体: ISO/TC307, IETF
  - 規制当局: 金融庁, 日本暗号資産取引業協会

暗号資産カストディアンのセキュリティ対策についての考え方

暗号資産カストディアンの利用者保護を主な目的とし、情報セキュリティ対策体制を構築する上での考え方を示す文書

- 初版は2018年2月から検討を開始。2018年10月に草案を作成、パブコメを実施。
- Living Standardとして更新していくことを予定。
- 文書はISO、IETFそれぞれで標準化文書として提案完了。
- 日本語版は第2版を公開中。



CG TF CRYPTOASSETS GOVERNANCE TASK FORCE

暗号資産カストディアンのセキュリティ対策についての考え方（案）

Cryptoassets Governance Task Force[1]

2020年7月3日

本ドキュメントはIETFにおいて、インターネットドラフトとして標準化提案されます。
本ドキュメントに対するすべてのコメントはIETF知的財産権ポリシ(NOTE WELL)に同意したものとみなされます。
Be aware that all contributions to our work fall under the "NOTE WELL" terms therein.

CGTFの取り組み

ISO/TC307

- Security management of digital asset custodians [1]
- ISO/TC307 WG2/JWG4にCGTFメンバーが多数参加

認定自主規制団体

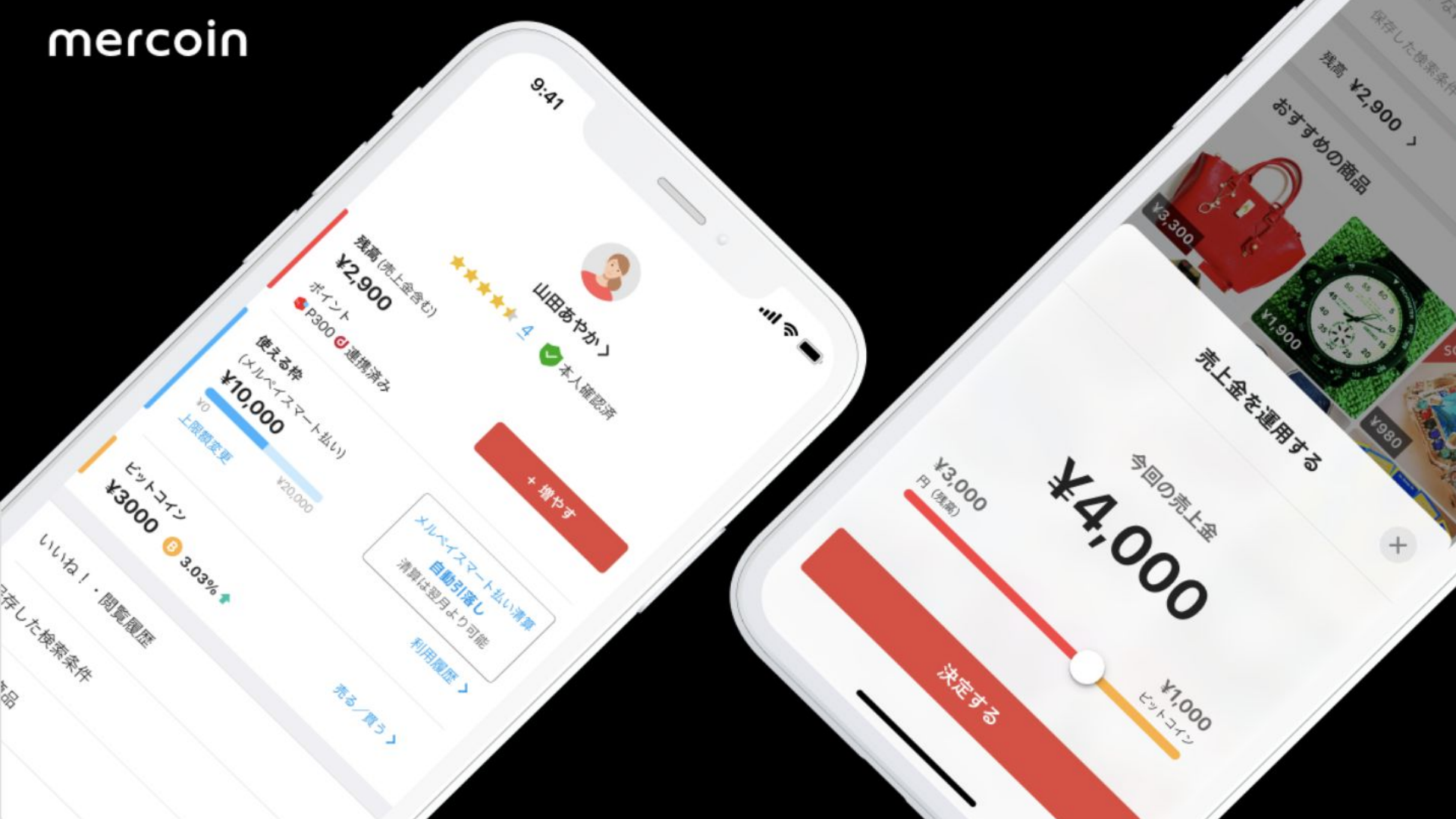
- 日本暗号資産取引業協会(JVCEA) 技術委員会に対するリエゾンの派遣

Internet Engineering Task Force (**IETF**)

- Sec WGの成果物をInternet-Draftとして投稿
- General Security Considerations for Cryptoassets Custodians [2]
- Terminology for Cryptoassets [3]
- 暗号資産のセキュリティに関するMailing-listの開設を予定

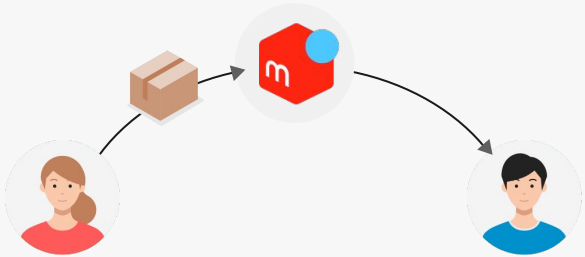
[1] Security management of digital asset custodians, ISO/TR 23576:2020
[2] General Security Considerations for Cryptoassets Custodians, draft-vcgtf-crypto-assets-security-considerations, Masashi Sato and Masaki Shimaoka and **Hirotaka Nakajima**
[3] Terminology for Cryptoassets, draft-nakajima-crypto-asset-terminology, **Hirotaka Nakajima** and Masanori Kusunoki and Keiichi Hida and Yuji Suga and Tatsuya Hayashi

mercoin

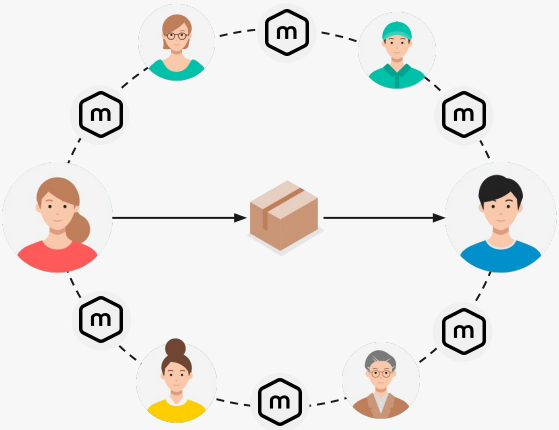

9:41
残高 (売上金含む)
¥2,900
ポイント
P300 連携済み
使える枠
(メルペイスマート払い)
¥10,000
¥0
上限額変更
¥20,000
ビットコイン
¥3000
3.03%
+ 増やす
山田あやか」
4
本人確認済
メルペイスマート払い清算
自動引落し
清算は翌月より可能
利用履歴
売る／買う」
いいね！・閲覧履歴
保存した検索条件
残高 ¥2,900」
おすすめの商品
¥3,300
¥1,900
¥980
売上金を運用する
今回の売上金
¥4,000
¥3,000
円 (残高)
¥1,000
ビットコイン
決定する

ブロックチェーン技術によって生まれる
分散型の新しいマーケットプレイス

メルカリを中心とした安心安全な取引
（モノ・お金）



お客さまが様々な形で参加・介入 する
新しい安心安全 で便利な取引
（モノ・お金＋無形のサービス・権利など）

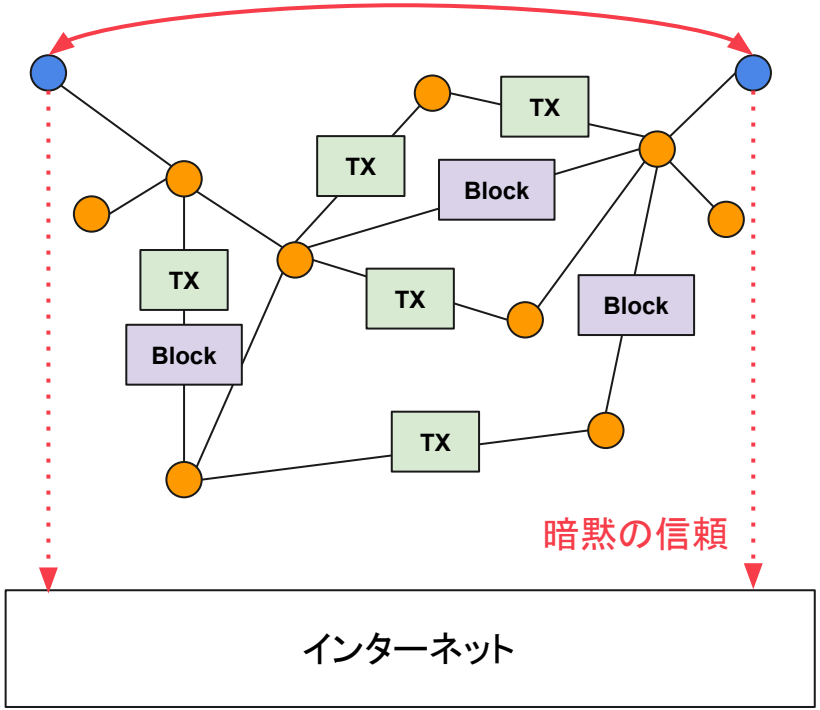


= メルカリのブロックチェーン技術

暗号資産の今後の課題(の一部)

Satoshiが信じていたもの

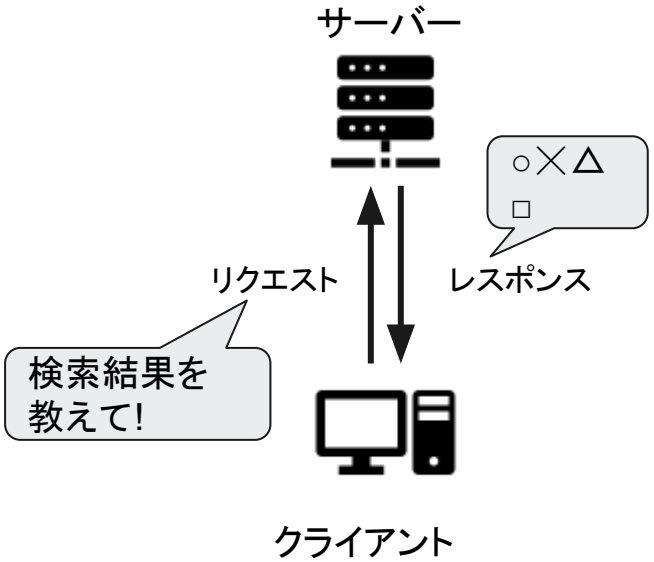
この2者間の取引において信頼する第三者が不要



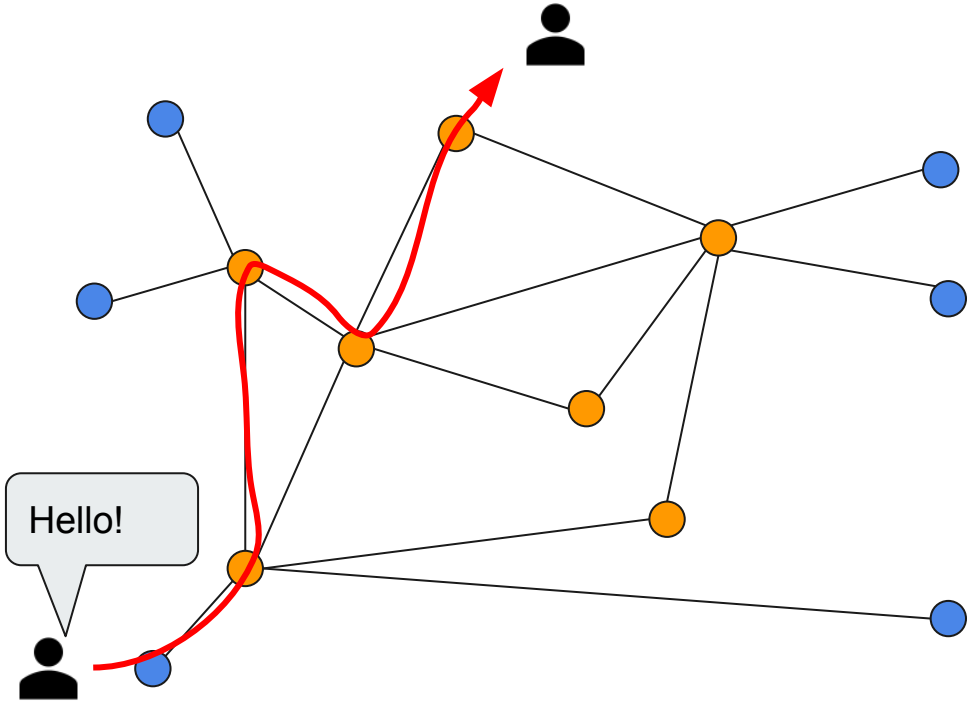
- ソフトウェアや開発者コミュニティ
  - BIPやEIP, ERCの中身を理解してアップデートしている?
- Underlay network
  - インターネットは十分に安全?

暗黙的に信頼していたシステムについても考える必要があるのではないか？

Peer-to-peerネットワーク

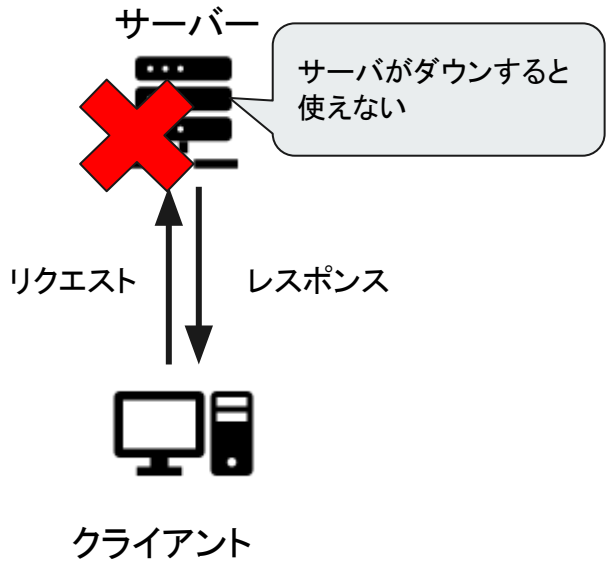


クライアント・サーバ型モデル

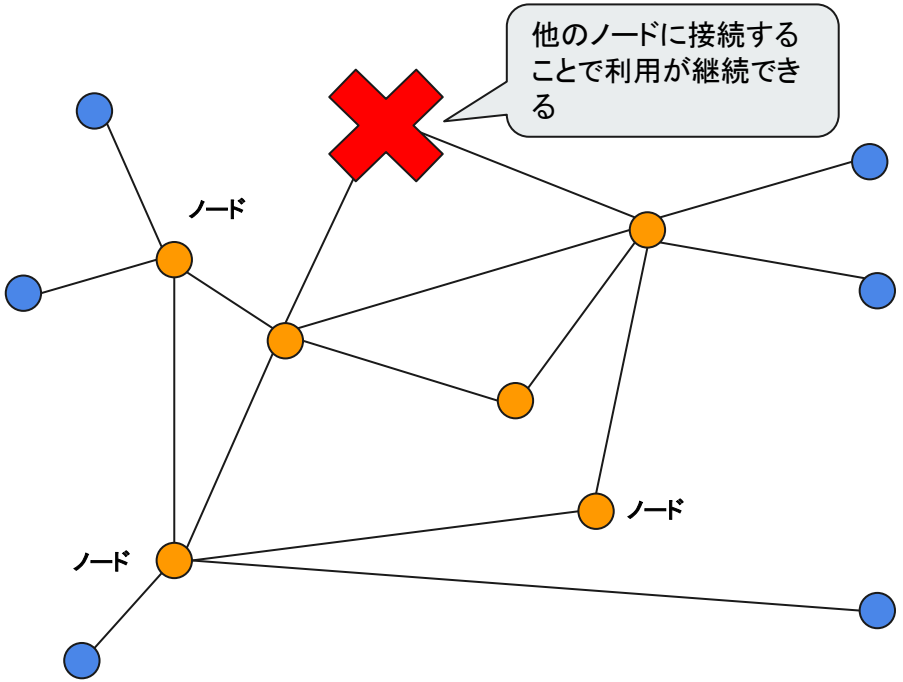


Peer-to-peerモデル

Peer-to-peerネットワーク

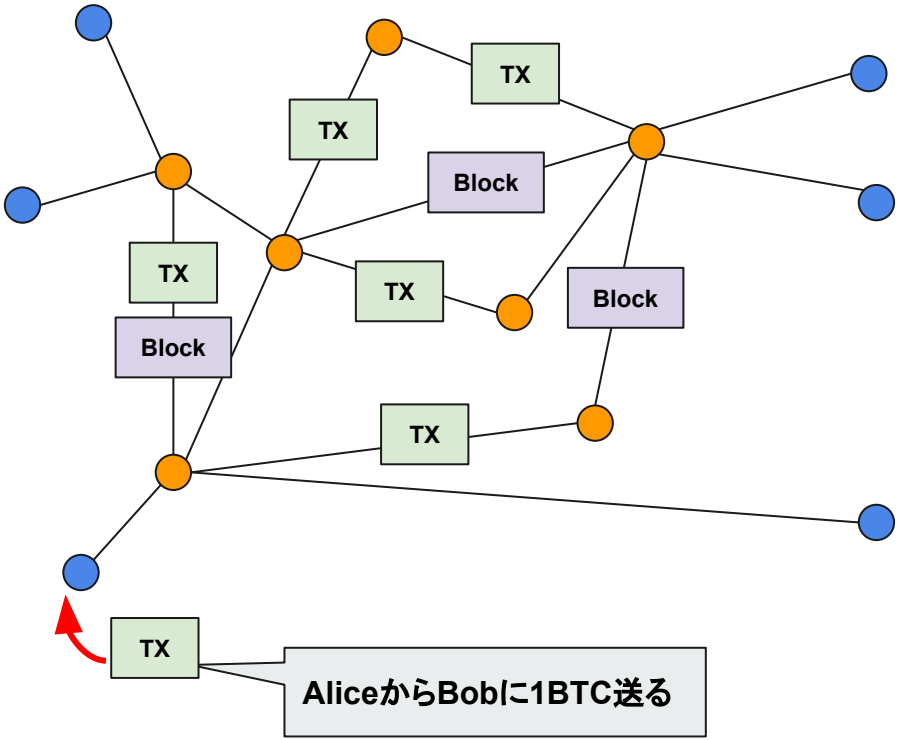


クライアント・サーバ型モデル



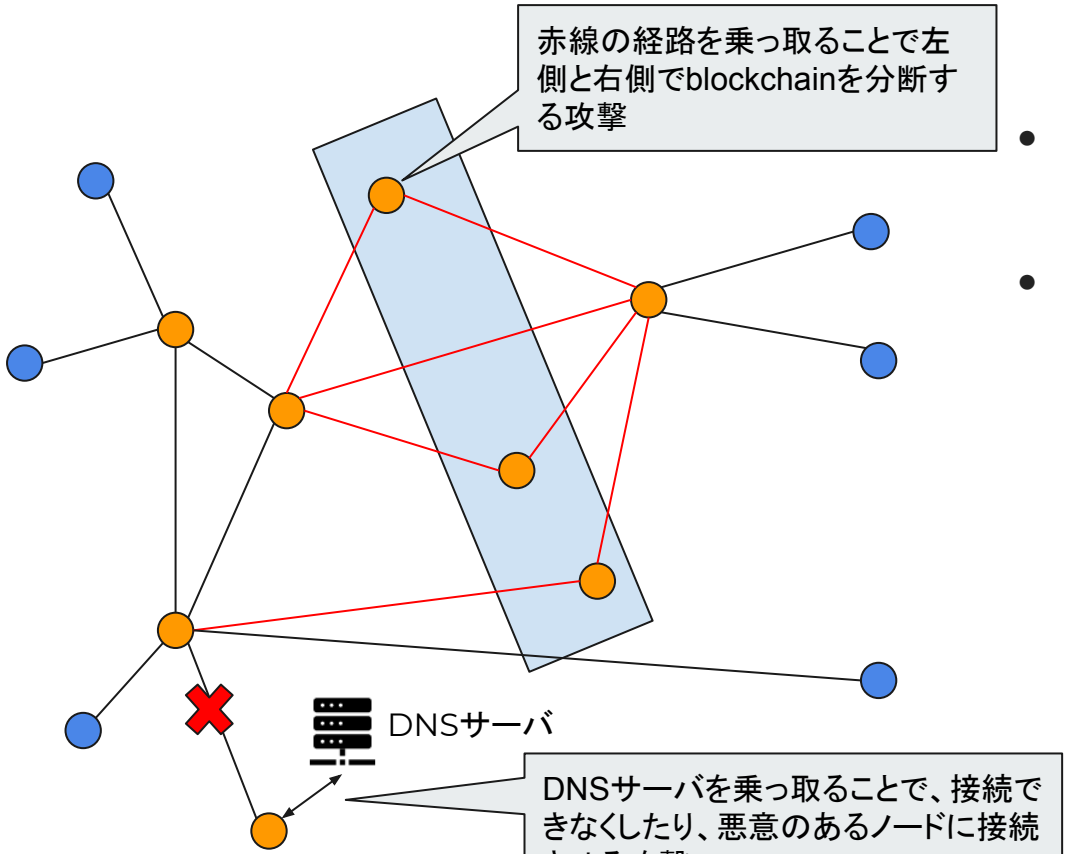
Peer-to-peerモデル

Blockchainのネットワーク



- BlockchainではP2P型モデルのネットワーク構造を取る
- すべてのノードにトランザクションとブロックが伝播される
- 1ノードは平均8ノードと接続している(Bitcoin)
- 初めて起動するときにはソースコードに書かれたDNSもしくはIPアドレスに接続する(bootstrap node)

ネットワークに対する攻撃

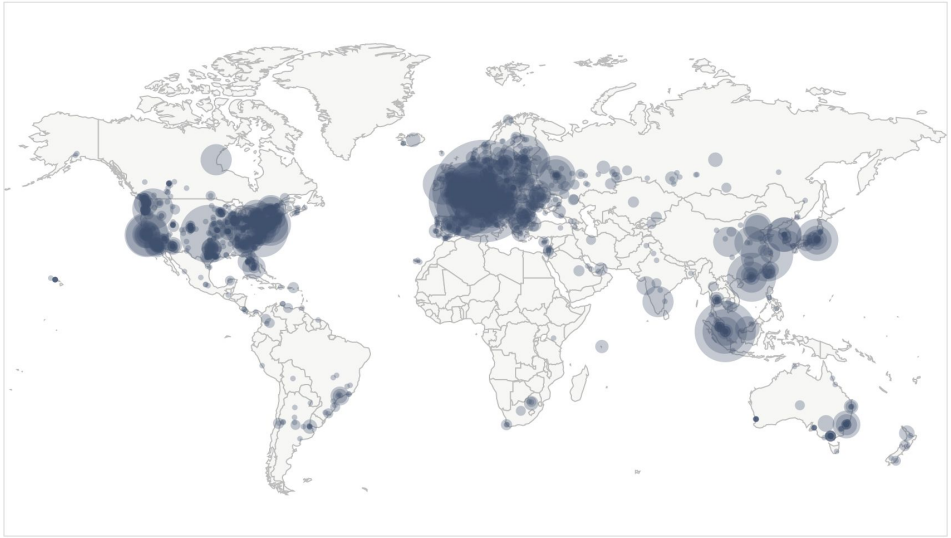


- ネットワーク上の経路を乗っ取ることにより、Blockchainネットワークを分断する攻撃 [Apostolaki, 2017]
- 初めて接続するノードの接続先に対する攻撃 [Faye, 2019]

インターネットは
Blockchainの安全性に密接に関係している

DNSSEC非対応のブートストラップノード
→ 44%
RPKIは果たして？

Bitcoinノード内訳

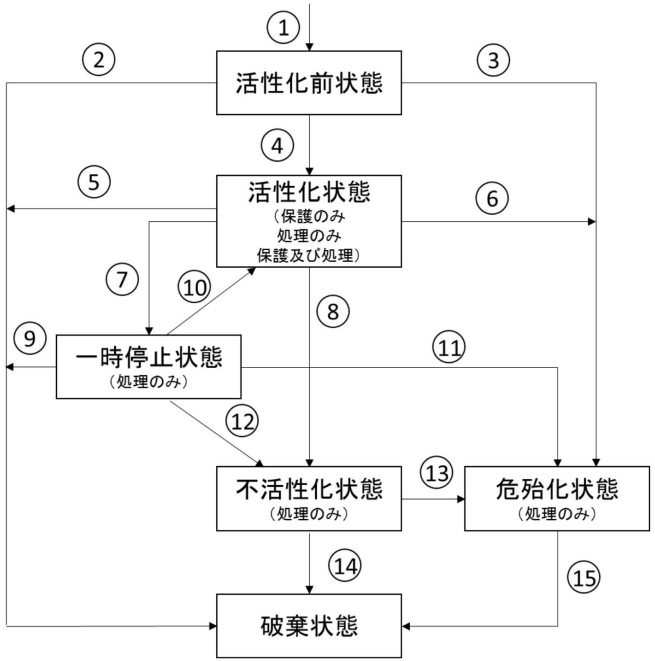


- 国別
  アメリカ(25.46%), ドイツ(20.00%), フランス(6.42%), オランダ (5.33%), シンガポール(3.72%)
  日本は10位(2.11%)
- ネットワーク別
  - Hetzner Online GmbH 1120 (11.87%)
  - Amazon.com, Inc. 819 (8.68%)
  - DigitalOcean, LLC 689 (7.30%)
  - OVH SAS 520 (5.51%)
  - Choopa, LLC 386 (4.09%)
  - **40%近くのノードが Public クラウド上で稼働**

果たして本当にDecentralizedなのだろうか？🤔

出典: https://bitnodes.earn.com/, 2020年現在

暗号鍵のライフサイクル



- 信頼できる第三者の不存在
  - 失効機能を有さない
  - 暗号鍵の危殆化≒資産の消失
- 危殆化した鍵から資産を回復する方法
  - トランザクションの巻き戻し
  - 奪取した攻撃者からの返還
- 暗号鍵の破棄も困難

[1] Barker, Elaine, et al. Recommendation for key management: Part 1: General. National Institute of Standards and Technology, Technology Administration, 2006.

ウォレット

- ハードウェアウォレット
  - 暗号資産で使用する署名鍵を格納する専用の電子機器
  - 一般的なHSM(Hardware Security Module)を利用できないケースが多く、認証プログラムも未整備
  - サプライチェーンリスク
- ソフトウェアウォレット
  - 安全でないウォレットアプリの存在 [2]

[1] Volotikin, S. "Software attacks on hardware wallets." Black Hat USA (2018).
[2] C. Li, D. He, S. Li, S. Zhu, S. Chan and Y. Cheng, "Android-based Cryptocurrency Wallets: Attacks and Countermeasures," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 9-16

ベストプラクティスが必要

- 規制当局の指針やCGTFのドキュメント等は”考え方”に過ぎず、実装については触れていない
  - 実装については個社に任されている
  - 悩む部分も非常に多い
  - 資産をカストディアンに預ける世界で本当に良いのか？
- Best Current Operational Practices [1]
  - インターネット(ネットワーク)での取り組み
  - こうした取り組みが暗号資産・ブロックチェーンであってもよいのではないだろうか。

[1] https://www.ietf.org/rfc/bcp-index.txt

まとめ

- 暗号資産交換所とカストディアンの関係
- 暗号資産セキュリティに取り組む活動の紹介
- 暗号資産の今後の課題
  - 暗号鍵管理
  - トラストアンカー